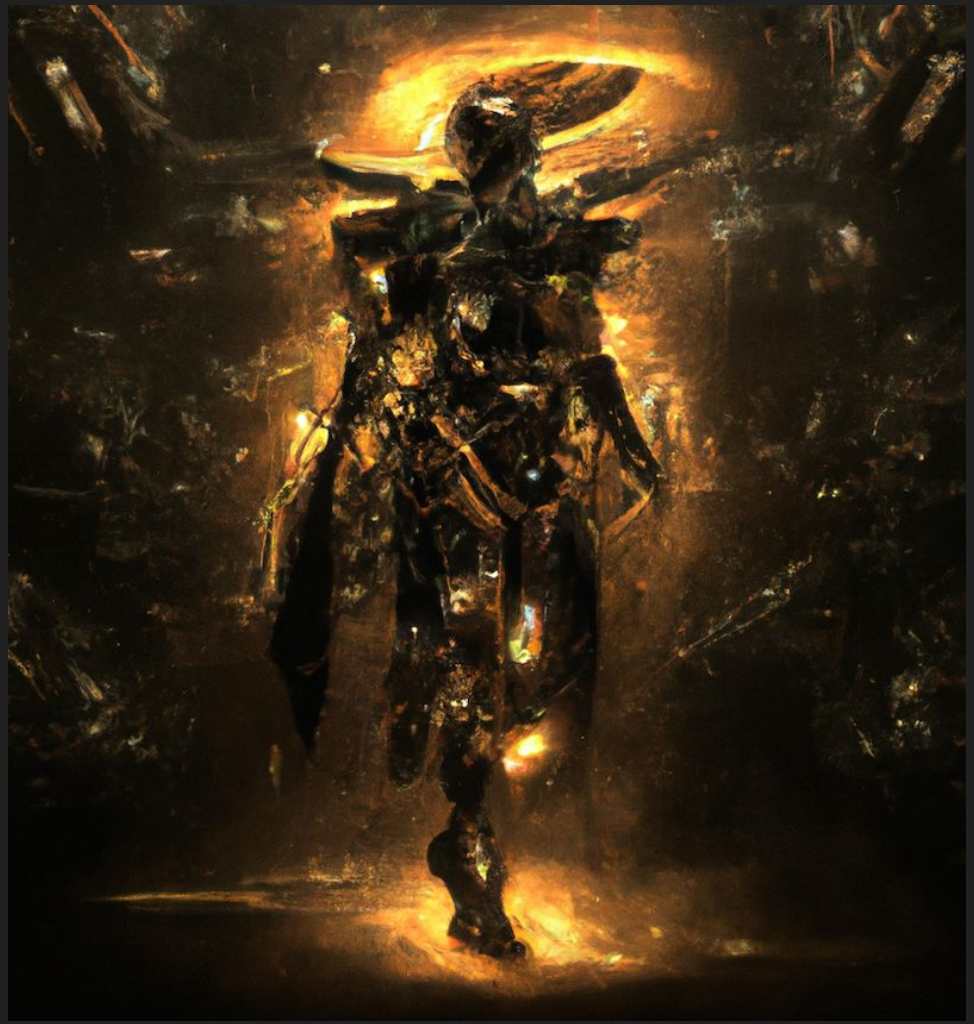
Influence operation 101 example

By

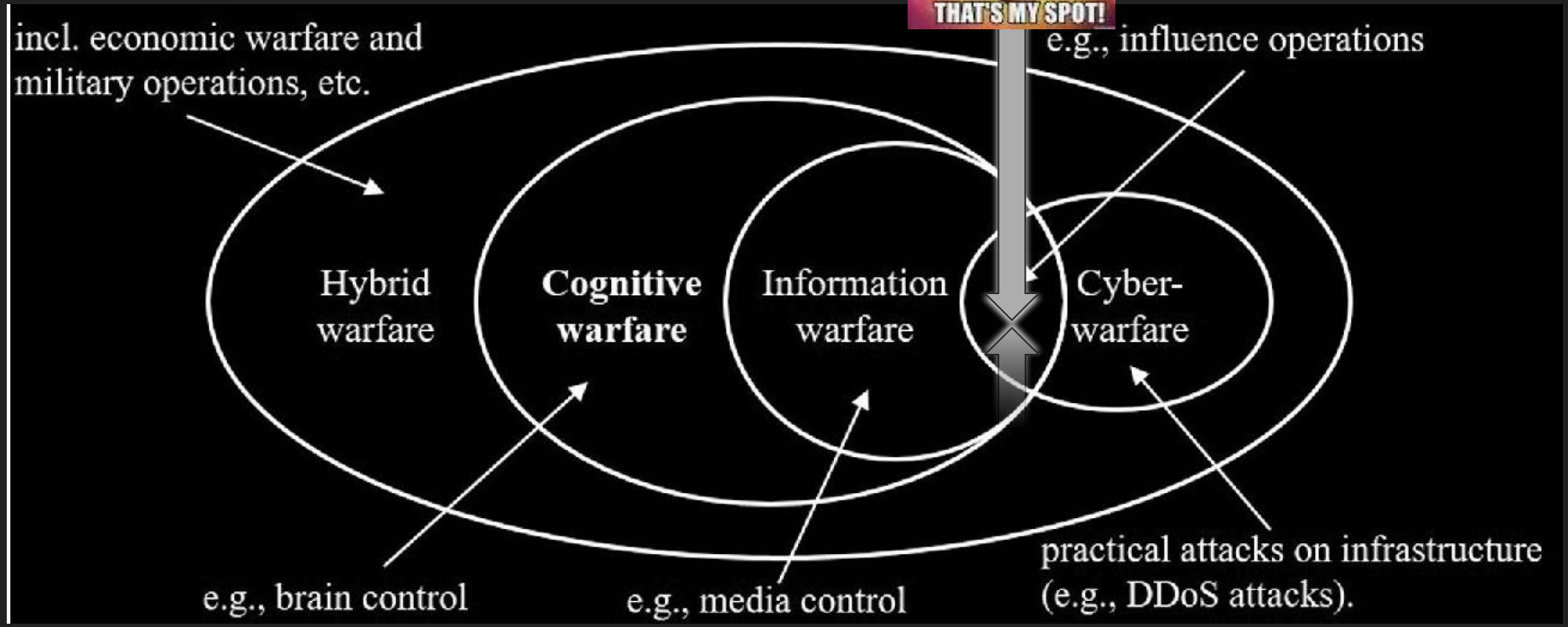
Jindrich Karasek aka **4n6strider**

TREND MICRO

TLP:Amber



What: (In theory)



Source: https://academic.oup.com/jogss/article/7/4/ogac016/6647447


TLP:Amber

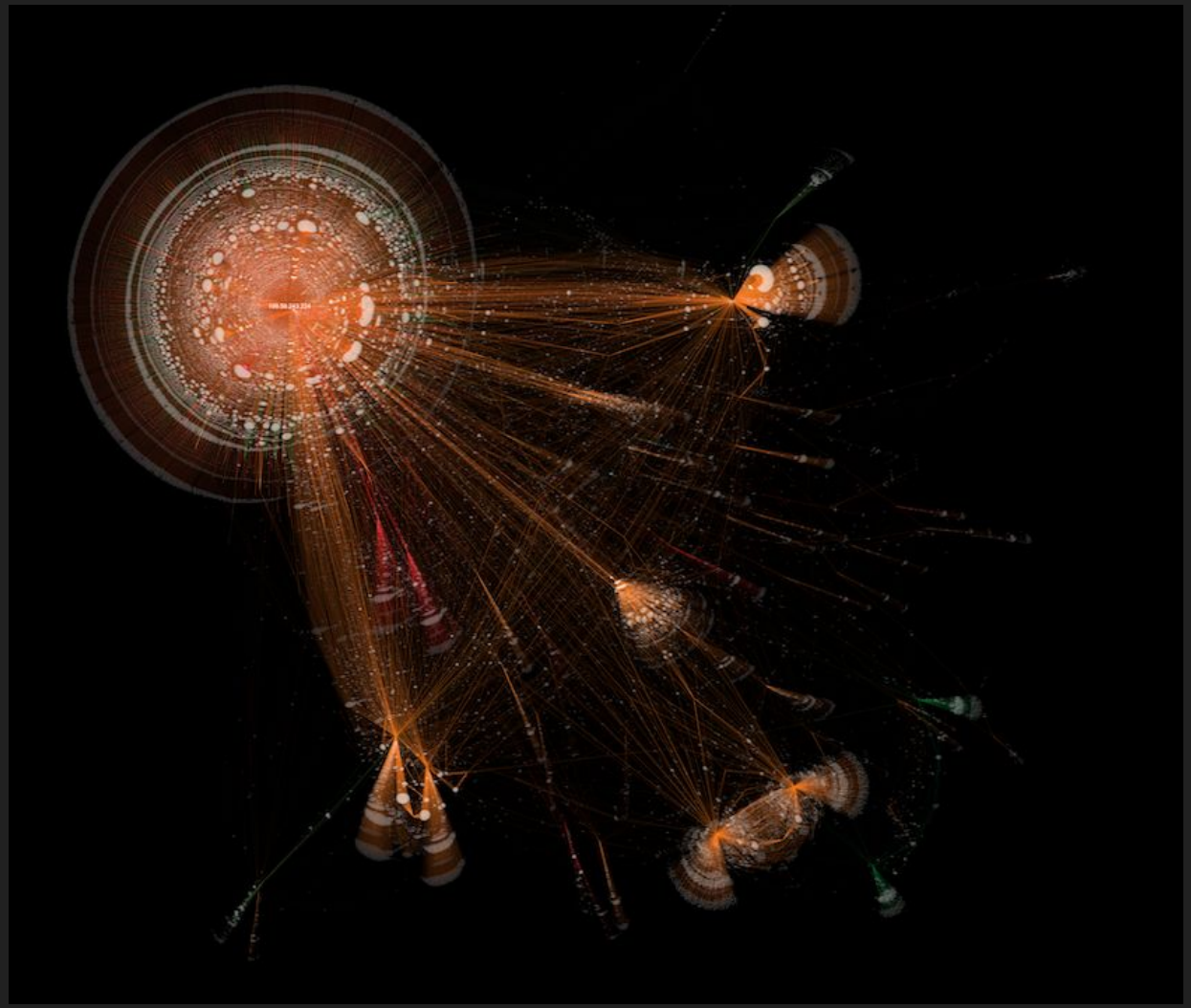
Dataset:

- 750 distinct URLs
- 430 domains
- 128 IPs
- 448 259 netflows
- 498 760 pDNS records

- Processed with Eolas

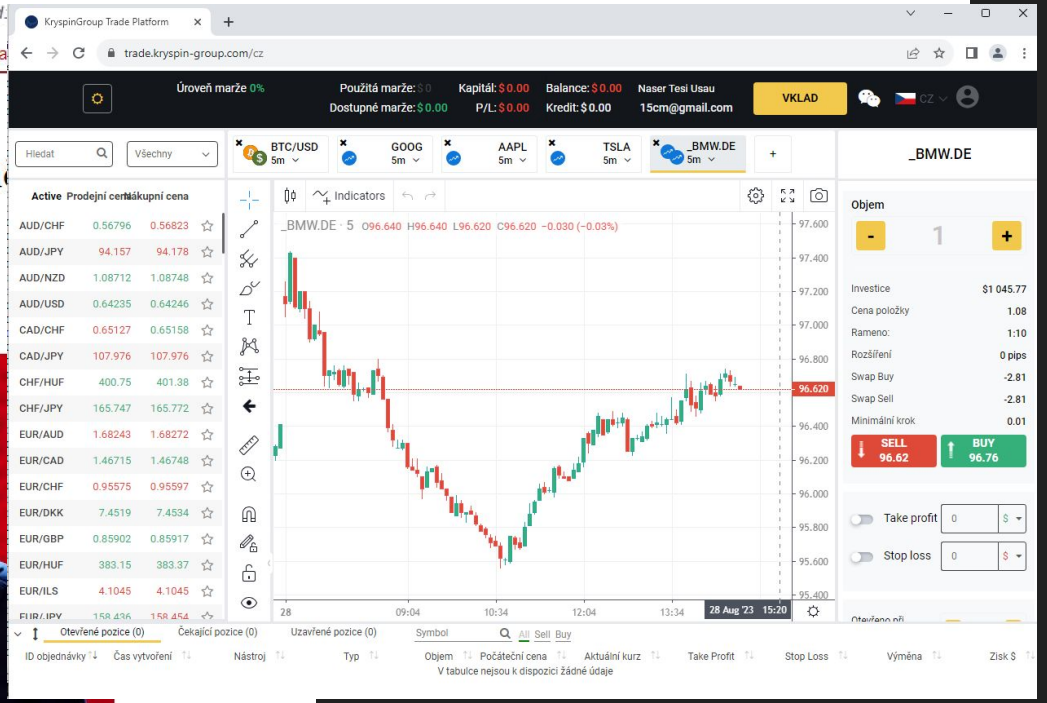
https://github.com/Eolas-bith/UNICRI-Decode-CW

TLP:Amber

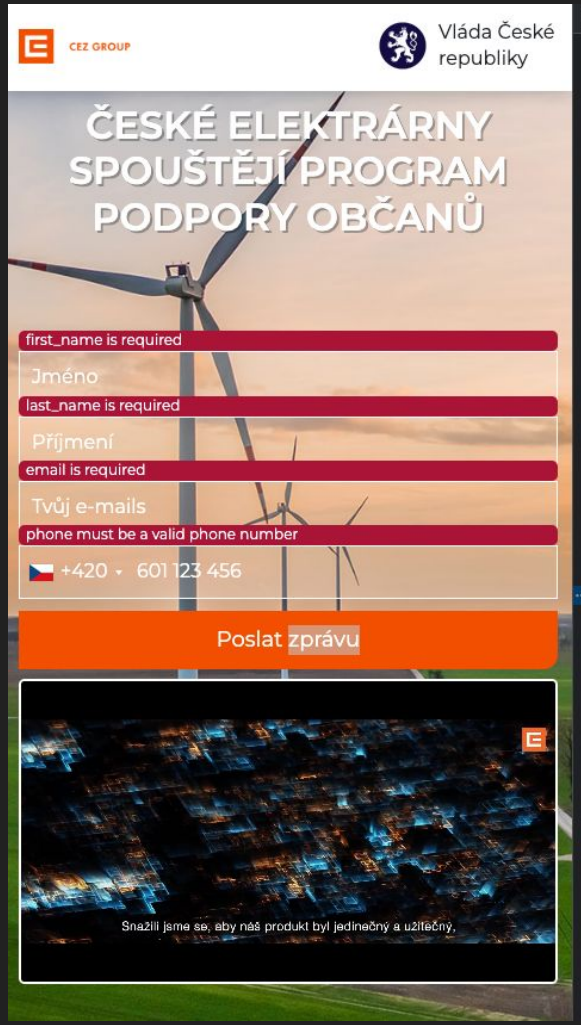


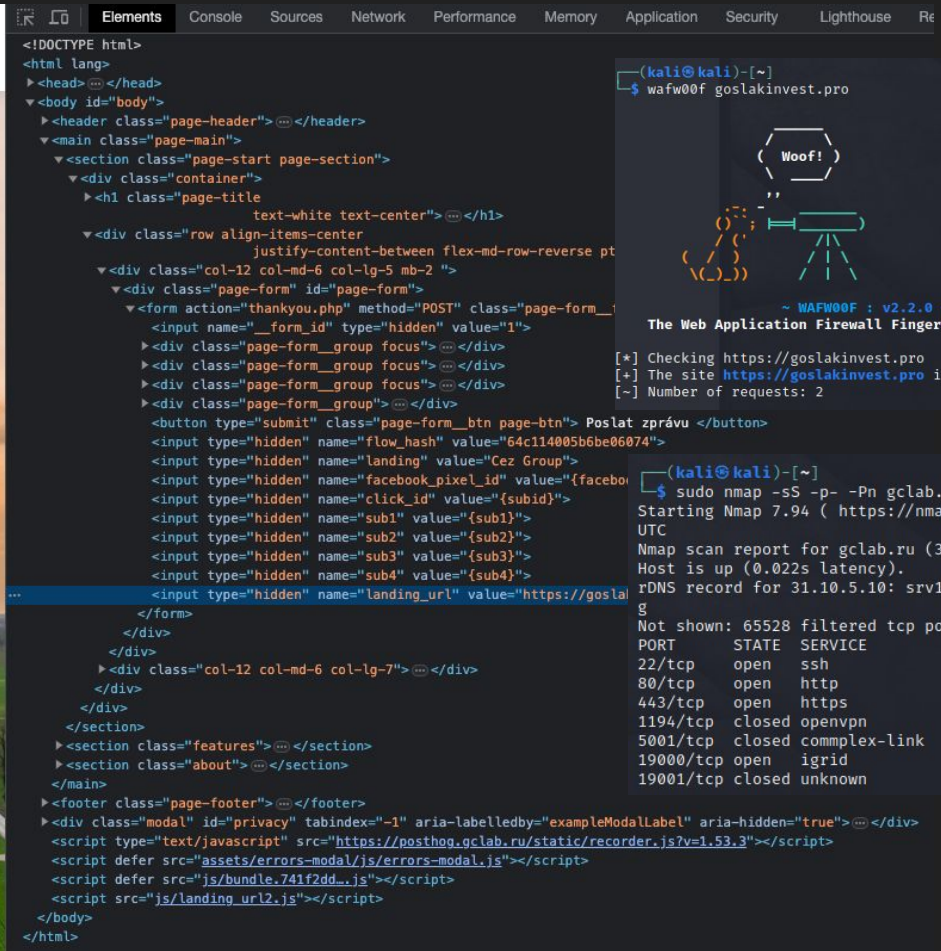
První zákon Petra Pavla o zajištění finan… zabezpečení občanů – přijat

pondělí 28. srpna 2023 – Praha
Lukáš Zacpal



TLP:Amber


CEZ GROUP
Vláda České republiky
ČESKÉ ELEKTRÁRNY SPOUŠTĚJÍ PROGRAM PODPORY OBČANŮ
first_name is required
Jméno
last_name is required
Příjmení
email is required
Tvůj e-mails
phone must be a valid phone number
+420
601 123 456
Poslat zprávu
Snažili jsme se, aby náš produkt byl jedinečný a užitečný.


Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
<!DOCTYPE html>
<html lang>
<head></head>
<body id="body">
<header class="page-header"></header>
<main class="page-main">
<section class="page-start page-section">

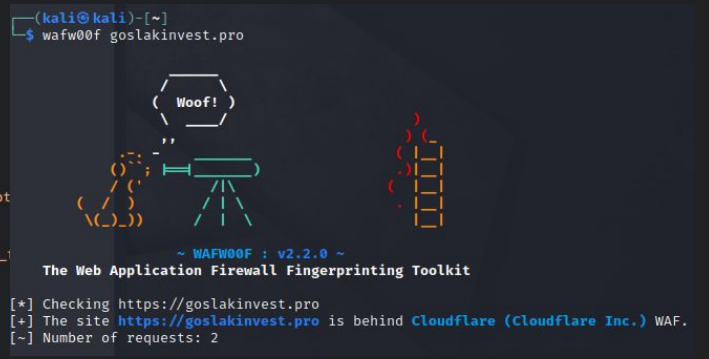
<h1 class="page-title
text-white text-center"></h1>
<div class="row align-items-center
justify-content-between flex-md-row-reverse pt

<form action="thankyou.php" method="POST" class="page-form__
<input name="__form_id" type="hidden" value="1">

<button type="submit" class="page-form__btn page-btn"> Poslat zprávu </button>
<input type="hidden" name="flow_hash" value="64c114005b6be06074">
<input type="hidden" name="landing" value="Cez Group">
<input type="hidden" name="facebook_pixel_id" value="{faceboo
<input type="hidden" name="click_id" value="{subid}">
<input type="hidden" name="sub1" value="{sub1}">
<input type="hidden" name="sub2" value="{sub2}">
<input type="hidden" name="sub3" value="{sub3}">
<input type="hidden" name="sub4" value="{sub4}">
<input type="hidden" name="landing_url" value="https://gosla
</form>

</section>
<section class="features"></section>
<section class="about"></section>
</main>
<footer class="page-footer"></footer>

<script type="text/javascript" src="https://posthog.gclab.ru/static/recorder.js?v=1.53.3"></script>
<script defer src="assets/errors-modal/js/errors-modal.js"></script>
<script defer src="js/bundle.741f2dd….js"></script>
<script src="js/landing_url2.js"></script>
</body>
</html>


(kali㉿kali)-[~]
$ wafw00f goslakinvest.pro
Woof!
~ WAFW00F : v2.2.0 ~
The Web Application Firewall Fingerprinting Toolkit
[*] Checking https://goslakinvest.pro
[+] The site https://goslakinvest.pro is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2

(kali㉿kali)-[~]
$ sudo nmap -sS -p- -Pn gclab.ru
Starting Nmap 7.94 (https://nmap.org) at 2023-08-22 14:01 UTC
Nmap scan report for gclab.ru (31.10.5.10)
Host is up (0.022s latency).
rDNS record for 31.10.5.10: srv17401.hosted-by-eurohoster.org
Not shown: 65528 filtered tcp ports (no-response)
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
443/tcp open https
1194/tcp closed openvpn
5001/tcp closed commplex-link
19000/tcp open igrid
19001/tcp closed unknown

TLP:Amber

Thank you!

Jindrich Karasek aka 4n6strider
Senior Cyber Threat Researcher at Trend Micro

Version: cd56e0d82428db36a6148644ef7a2ae3592512d0

https://linktr.ee/4n6strider